

---

# **IAW - Práctica - Hardening WordPress**

IAW - Implantación de Aplicaciones Web

# Índice general

<b>1</b>	<b>Práctica: Hardening WordPress</b>	<b>1</b>
1.1	Qué acciones podemos realizar para mejorar la seguridad de un sitio WordPress . . . . .	1
1.2	Entregables . . . . .	1
<b>2</b>	<b>Referencias</b>	<b>3</b>
<b>3</b>	<b>Licencia</b>	<b>4</b>

# 1 Práctica: Hardening WordPress

En esta práctica tendremos que mejorar la seguridad de un sitio web [WordPress](#).

Puede hacer uso de la guía [21 Trucos para tener tu WordPress seguro](#) de la empresa [SiteGround](#).

## 1.1. Qué acciones podemos realizar para mejorar la seguridad de un sitio WordPress

- Cambiar el prefijo de las tablas de la base de datos.
- Configurar las claves de seguridad de Wordpress (Keys y Salt).
- No utilizar nombres como `admin` o `administrador`.
- Deshabilitar las notificaciones de pingbacks y trackbacks en el panel de administración.
- Bloquear con archivos `.htaccess` el acceso a archivos importantes del sitio web (`wp-config.php`, etc.)
- Bloquear que el servidor web muestre un listado con el contenido de un directorio.
- Modificar los permisos de los archivos y directorios. Los archivos deben ponerse a 644 y los directorios a 755.
- Bloquear la ejecución de código PHP en los siguientes directorios: `wp-content/uploads`, `wp-content/plugins` y `wp-content/themes`.
- Deshabilitar la edición de ficheros desde el panel de administración de WordPress.
- Deshabilitar las sugerencias de inicio de sesión.
- Instalar un plugin que permita modificar la ruta de acceso del panel de administración.
- Desactivar el acceso al archivo `xmlrpc.php` con reglas en un archivo `.htaccess`.
- Ocultar la información de las cabeceras que envía el servidor web con la versión del servidor y PHP.

## 1.2. Entregables

En esta práctica habrá que entregar un **documento técnico** con la descripción de los pasos que se han llevado a cabo durante todo el proceso.

El documento debe incluir **como mínimo** lo siguientes contenidos:

- URL del repositorio de GitHub donde se ha alojado el documento técnico escrito en [Markdown](#).
- Script de `bash` para automatizar las acciones que pueda para mejorar la seguridad del sitio web.

- Descripción y captura de pantalla de todos los pasos que ha realizado para mejorar la seguridad de WordPress.

## 2 Referencias

- [WordPress](#)
- [Blog sobre administración de sistemas WordPress.](#)
- [21 Trucos para tener tu WordPress seguro](#) de la empresa [SiteGround](#).
- [Curso de Ciberseguridad en WordPress.](#) OpenWebinars.

## **3 Licencia**

Esta página forma parte del curso Implantación de Aplicaciones Web de José Juan Sánchez y su contenido se distribuye bajo una licencia Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional.